UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,752	10/31/2001	Richard H. Harris	RPS920010068US1	3546

7590 01/14/2004

SAWYER LAW GROUP
P.O. Box 51418
Palo Alto, CA 94303

EXAMINER	
AU, SCOTT D	

ART UNIT	PAPER NUMBER
2635	

DATE MAILED: 01/14/2004

4

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/002,752	HARRIS, RICHARD H.	
	Examiner	Art Unit	
	Scott Au	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-16 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-16 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 31 October 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

The application of Harris et al. for a "Secure smart card" filed October 31, 2001 has been examined.

Claims 1-16 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2 and 6 are rejected under 35 U.S.C. 102(b) as being anticipated by Lessin et al. (US# 4,868,376).

Referring to claim 1, Lessin et al. disclose a method for providing a secure transaction, comprising the steps of:

(a) receiving a new identification (i.e. new PIN) verification data by a transaction device (10) (i.e. a programmable intelligent transaction card) directly from a user (i.e. note process of programming new PIN) (col. 13 lines 20-43);

(b) storing the new identification verification data on the transaction device only, wherein the new identification verification data is not shared with another device (col. 13 lines 44-48; see Figures 1A and 15C);

(c) receiving an input of an identification verification data by the transaction device directly from the user (i.e. user uses new PIN) (col. 5 lines 15-24);

(d) activating the transaction device if the inputted identification verification data matches the new identification verification data (col. 10 lines 2-5; see Figure 11); and

(e) deactivating the transaction device when an event occurs (i.e. routine exited) (col. 8 lines 27-38).

Referring to claim 2, Lessin et al. disclose the method of claim 1, wherein the receiving step (a) comprises:

(a1) assigning an initial identification verification data to the user (i.e. current PIN of the user);

(a2) receiving the initial identification verification data by the transaction device directly from the user (i.e. step 860);

(a3) verifying the initial identification verification data by the transaction device (i.e. step 862);

(a4) receiving an indication of a new identification verification data by the transaction device (i.e. step 872); and

(a5) receiving the new identification verification data by the transaction device directly from the user (i.e. step 878) (col. 13 lines 20-48; see Figure 15C).

Referring to claim 6, Lessin et al. disclose the method of claim 1 wherein the new identification verification data comprises at least one of the following:

a personal identification number ;a fingerprint; or a signature (col. 4 lines 7-11).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 9-10 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wallerstein (US# 5,585,787) in view of Mears (US# 5,539,400).

Referring to claim 9, Wallerstein discloses a transaction device, comprising: an inputting means (52) (i.e. a keyboard controller circuit) for receiving an inputted identification verification data (i.e. identification number) (col. 6 lines 7-8); a processor (40) (i.e. central processing unit) coupled to the decoder (i.e. a decoder is built-in of a CPU), wherein the decoder asserts an activation signal to the processor (40) if the identification verification data is verified, wherein the decoder de-asserts the activation signal when an event occurs (col. 6 lines 9-28; see Figure 4). However, Wallerstein did not explicitly disclose a decoder coupled to the inputting means for sensing, decoding, and verifying the inputted identification verification data.

In the same field of endeavor of decoding device, Mears discloses a decoder (90) (i.e. an encoder logic) coupled to the inputting means (52) (i.e. keypad array) for

sensing, decoding, and verifying the inputted identification verification data (col. 4 lines 9-19;see Figures 1-2 and 4) in order to analyze the keypad array input logic when one of the sensor circuit detect a depressed key.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include an encoder logic coupled to the keypad arrayfor sensing, detecting, and verifying a depressed key disclosed by Mears between the input control and a CPU of Wallerstein with the motivation for doing so would allow faster for the CPU to process and more reliable in order to improve transaction device operate efficiently.

Referring to claim 10, Wallerstein in view of Mears disclose the device of claim 9. Wallerstein discloses wherein the event comprises a completion of a secure transaction (col. 3 lines 1-19; see Figure 5).

Referring to claim 12, Wallerstein in view of Mears disclose the device of claim 9. Mears discloses wherein the inputting means comprises a plurality of capacitive keys, wherein each capacitive key comprises a first side and a second side (col. 3 lines 17-29; see Figures 2 and 4) where is coupled to oscillator on one side and coupled to the decoder (90) (i.e. encoder function as a decoder) on the second side.

Referring to claim 13, Wallerstein in view of Mears disclose the device of claim 9, Mears discloses further comprising: an oscillator (70) (i.e. an oscillator) coupled to the inputting means (52) (i.e. keypad array); and

a power source (62) (i.e. battery) coupled to the oscillator (70) (i.e. an oscillator) and the decoder (90) (i.e. an encoder functions as a decoder) (col. 3 lines 17-29 and col. 4 lines 9-19; see Figures 1-2 and 4).

Referring to claim 14, Wallerstein in view of Mears disclose the device of claim 9. Wallerstein discloses wherein the decoder (40) (i.e. CPU also function as a decoder that can verify the data, stored data in memory and determining identification data matches) comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data (col. 6 lines 9-28).

Claims 3-4 and 7 are rejected under 35 U.S.C 103(a) as being unpatentable over Lessin et al. (US# 4,868,376) in view of Grant et al. (US# 6,095,416).

Referring to claim 3, Lessin et al. disclose the method of claim 1, wherein the activating step (d) comprises:

(dl) determining if the inputted identification verification data matches the new identification verification data by the transaction device (i.e. step 124);

(d2) activating the transaction device if the inputted identification verification data matches the new identification verification data (i.e. step 128) (col. 5 lines 15-24; see Figure 4). However, Lessin et al. did not explicitly disclose step:

(d3) starting a timer if the transaction device is activated, wherein the timer expires after the predetermined period of time.

In the same field of endeavor of method and device for preventing unauthorized use of credit cards, Grant et al. disclose step: starting a timer if the transaction device is activated, wherein the timer expires after the predetermined period of time (col. 3 lines 59-62) in order to disable the transaction after a predetermined limited of time to prevent a fraudulent transaction.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include step: starting a timer if the transaction device is activated, wherein the timer expires after the predetermined period of time of credit cards method and system disclosed by Grant et al. into portable interactive personal data system of Lessin et al. with the motivation for doing so would allow the transaction to deactivate after a predetermined limited of time to prevent fraudulent transaction.

Referring claim 4, Grant et al. disclose the method of claim 3, wherein the deactivating step (e) comprises:

(e1) deactivating the transaction device when the timer expires (col. 3 lines 59-62).

Referring to claim 7, Lessin et al. disclose a method for providing a secure transaction, comprising the steps of:

(a) receiving an initial identification verification data by the transaction device directly

from the user (i.e. step 860);

(b) verifying the initial identification verification data by the transaction device (i.e. step 862);

(c) receiving a new identification verification data by the transaction device directly from the user (i.e. step 878) (col. 13 lines 20-48; see Figure 15C);

(d) storing the new identification verification data on the transaction device only, wherein the new identification verification data is not shared with another device (col. 3 lines 7-27 and col. 13 lines 20-48; see Figures 1A and 15C);

(e) receiving an input of an identification verification data by the transaction device directly from the user (col. 5 lines 15-24);

(f) determining if the inputted identification verification data matches the new identification verification data by the transaction device (col. 5 lines 15-24);

(g) activating the transaction device if the inputted identification verification data matches the new identification verification data (col. 5 lines 15-24).

However, Lessin et al. did not explicitly disclose step:

(h) starting a timer if the transaction device is activated, wherein the timer expires after a predetermined period of time; and

(i) deactivating the transaction device when the timer expires.

In the same field of endeavor of method and device for preventing unauthorized use of credit cards, Grant et al. disclose steps:

(h) starting a timer if the transaction device is activated, wherein the timer expires after a predetermined period of time; and

(i) deactivating the transaction device when the timer expires (col. 3 lines 59-62) in order to disable the transaction after a predetermined limited of time so that it cannot be used for a fraudulent transaction.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include steps: starting a timer if the transaction device is activated, wherein the timer expires after a predetermined period of time; and deactivating the transaction device when the timer expires of credit cards method and system disclosed by Grant et al. into portable interactive personal data system of Lessin et al. with the motivation for doing so would allow the transaction to deactivate after a predetermined limited of time to prevent fraudulent transaction.

Claim 5 is rejected under 35 U.S.C 103(a) as being unpatentable over Lessin et al. (US# 4,868,376) in view of Herwig (US# 2002/0082925).

Referring to claim 5, Lessin et al. disclose the method of claim 1. However, Lessin et al. did not explicitly disclose wherein the deactivating step (e) comprises:

(el) deactivating the transaction device when the secure transaction is completed.

In the same field of endeavor of method and apparatus for utilizing a smart card, Herwig discloses deactivating the transaction device when the secure transaction is completed (page. 4 paragraph 38) in order to have a secured retail transaction account.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include step: deactivating the transaction device

when the secure transaction is completed of method and apparatus for utilizing a smart card disclosed by Herwig into portable interactive personal data system of Lessin et al. with the motivation for doing so would allow the transaction device to deactivate after a transaction is completed.

Claim 8 is rejected under 35 U.S.C 103(a) as being unpatentable over Lessin et al. (US# 4,868,376) in view of Grant et al. (US# 6,095,416) and in further view of Herwig (US# 2002/0082925).

Referring to claim 8, Lessin et al. in view of Grant et al. and Herwig disclose a method of claims 5 and 7, as evident by claim 8 being equivalent to that the combine of claim 5 and claim 7 "steps a-g" addressed above, incorporated herein. Therefore, claim 8 is rejected for the same reasons given with respect to claims 5 and 7 "steps a-g" combined.

Claim 11 is rejected under 35 U.S.C 103(a) as being unpatentable over Wallerstein (US# 5,585,787) in view Mears (US# 5,539,400) and in further view of Suzuki (US# 4,801,787).

Referring to claim 11, Wallerstein in view of Mears disclose the device of claim 9. However, Wallerstein in view of Mears did not explicitly disclose further comprising:

a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

In the same field of endeavor of IC card identification system, Suzuki teaches a timer circuit (21T) (i.e. a timer circuit) coupled to the decoder (31) (i.e. a comparator), wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor (21) (i.e. CPU within system control section) when the timer circuit expires (col. 2 lines 19-29, 51-56 and col. 4 lines 3-10; see Figures 2 and 3) in order to prevent a fraudulent transaction.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires of IC card identification system disclosed by Suzuki into transaction system of Wallerstein in view of Mears with the motivation for doing so would allow the a transaction to deactivate after a predetermined limited of time to prevent a fraudulent transaction.

Claims 15-16 are rejected under 35 U.S.C 103(a) as being unpatentable over Mears (US# 5,539,400) in view of Wallerstein (US# 5,585,787) and further in view of Suzuki (US# 4,801,787).

Referring to claim 15, Mears discloses a transaction device (50) (i.e. system of transaction device), comprising:

a plurality of capacitive keys for inputting an identification verification data, wherein each capacitive key comprises a first side and a second side (col. 3 lines 17-29; see Figures 2 and 4); an oscillator (70) (i.e. an oscillator) coupled to the first side of each capacitive key; a decoder (90) (i.e. an encoder functions as a decoder) coupled to the second side of each capacitive key for sensing, decoding, and verifying the inputted identification verification data when the first and second sides of at least one of the capacitive keys are coupled; a power source (62) (i.e. battery) coupled to the oscillator(70) (i.e. an oscillator) and the decoder (90) (i.e. an encoder functions as a decoder) (col. 3 lines 17-29 and col. 4 lines 9-19; see Figures 1-2 and 4).

However, Mears did not explicitly disclose wherein the decoder comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data; a processor coupled to the decoder, wherein the decoder asserts an activation signal to the processor if the inputted identification verification data is verified; and a timer circuit coupled to the

decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

In the same field of endeavor of programmable credit card system, Wallerstein discloses wherein the decoder (40) (i.e. CPU able to do the decoding process) comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data; a processor coupled to the decoder (i.e. CPU also works as a decoder), wherein the decoder asserts an activation signal to the processor if the inputted identification verification data is verified (col. 6 lines 9-28; see Figure 4) in order to have a secured transaction.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include the decoder comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data; a processor coupled to the decoder, wherein the decoder asserts an activation signal to the processor if the inputted identification verification data is verified of programmable credit card system disclosed by Wallerstein into transaction system of Mears with the motivation for doing so would allow data is verified, sensed , decoded and stored when the transaction is processed.

However, Mears in view of Wallerstein did not explicitly disclose a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

In the same field of endeavor of IC card identification system, Suzuki teaches a timer circuit (21T) (i.e. a timer circuit) coupled to the decoder (31) (i.e. a comparator), wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor (21) (i.e. CPU within system control section) when the timer circuit expires (col. 2 lines 19-29, 51-56 and col. 4 lines 3-10; see Figures 2 and 3) in order to prevent fraudulent transaction.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires of IC card identification system of Suzuki into transaction system of Wallerstein and Suzuki with the motivation for doing so would allow the transaction to deactivate after a predetermined limited of time to prevent fraudulent transaction.

Referring to claim 16, Mears in view of Wallerstein and in further view of Suzuki disclose a transaction device, to the extent of claim 15 above, Wallerstein discloses the decoder de-asserts the activation signal to the process when a secure transaction is completed (col. 6 lines 9-28 and col. 7 lines 27-37; see Figure 5). Therefore, one skilled in the art understand that the (40) CPU of Wallerstein functions as a processor and a decoder where signal is de-asserted to the CPU when a secure transaction is completed.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Stuckert (US# 4,277,837) discloses a personal portable terminal for financial transactions.

Nagata et al. (US# 4,959,788) disclose IC card with keyboard for prestoring transaction data.

Any inquiry concerning this communication or earlier communications form the examiner should be directed to Scott Au whose telephone number is (703) 305-4680. The examiner can normally be reached on Mon-Fri, 8:30AM – 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached at (703) 305-4704. The fax phone numbers for the organization where this application or proceeding is assigned are (703)-

872-9314 for regular communications and (703)-872-9315 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)-305-3900.

Scott Au

SA

MICHAEL HORABIK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600